UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Civil Action No. _____

TULLIA HEISSENBERG, an individual,

Plaintiff,

v.

CELL NATION OF 3006 BROADWAY CORP., a New York corporation;
AKRAM INVESTMENTS, LLC, a Florida limited liability company;
INSTA MOBILITY, INC., a Florida corporation;
MELBER, LLC d/b/a HELLO UNLIMITED, an Oklahoma limited liability company;
LAXCA DF, INC. d/b/a FIVESTONE WIRELESS a/k/a DF WIRELESS, a California corporation;
and WIRELESS PCS METRO STATIONS, INC., a California corporation;

Defendant.
_____/

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Plaintiff TULLIA HEISSENBERG, an individual (hereafter referred to as "Plaintiff"), by and through undersigned counsel, hereby sues Defendants CELL NATION OF 3006 BROADWAY CORP., a New York corporation; AKRAM INVESTMENTS, LLC, a Florida limited liability company; INSTA MOBILITY, INC., a Florida corporation; MELBER, LLC d/b/a HELLO UNLIMITED, an Oklahoma limited liability company; FIVESTONES WIRELESS, a California corporation; and WIRELESS PCS METRO STATIONS, INC., a California corporation; for damages and equitable relief. As grounds therefor, Plaintiff alleges the following:

PRELIMINARY STATEMENT

1. This action is brought by Plaintiff, a retired senior citizen who lost approximately Three Million Dollars ($3,000,000.00) worth of cryptocurrency in an ongoing identity theft crime called "SIM swapping" or "SIM hijacking."

2. "SIM swapping" is not merely an ongoing crime; it is a booming crime -- especially one that targets cryptocurrency investors.

3. Over the past three years alone, undersigned counsel has represented nearly three hundred (300) victims of unauthorized SIM swapping across the country whose individual cryptocurrency losses have ranged from as little as $3,000.00 to as much as $12,500,000.00.

4. Of those 300-or-so cases, few if any represent stories as egregious as the targeted crime committed upon Plaintiff; as she was SIM swapped not once, not twice, not three times, but seven times over a six-month period before the criminal actors succeeded in stealing her cryptocurrency assets.[1]

5. Defendants are all Authorized Dealers who operate retail store locations under the brand of telecommunications provider Metro by T-Mobile -- the telecom provider through whom Plaintiff received her monthly cellphone service.

6. Documents maintained by Metro by T-Mobile and by Defendants demonstrate that employees or employee credentials at Defendant store locations were used to effectuate one or more of the unauthorized SIM swaps imposed upon Plaintiff -- each of which were vital in the scheme to steal Plaintiff's assets.

7. But for the Metro by T-Mobile Authorized Dealers' intentional participation in the scheme or their recklessness and gross negligence in failing to adequately protect employee credentials and Plaintiff's personal identifying information/Metro by T-Mobile account, Plaintiff would not have suffered the harm that she did.

8. Plaintiff brings this lawsuit to compensate her for her losses.

[1] Adding further insult to Plaintiff's injuries, she was also SIM swapped two more times by representatives at Metro by T-Mobile Authorized Dealer stores in Tulsa, OK and Orlando, FL, respectively (both owned and operated by Crysberg, Inc., a Metro agent and Authorized Dealer) in the two weeks following the multi-million dollar crime set forth herein.

PARTIES, JURISDICTION AND VENUE

THE PARTIES

Plaintiff

9. Plaintiff TULLIA HEISSENBERG is an individual domiciled in Delray Beach, Florida, is a citizen of the state of Florida, and is *sui juris*. At all times relevant hereto, Plaintiff was an accountholder and subscriber with Metro by T-Mobile. Among other things, Plaintiff's subscription with Metro by T-Mobile permitted Plaintiff to use her cellphone for the following -- all of which Plaintiff in fact did with her phone: make and receive telephone calls with people around the world, send and receive text messages with people around the world, and access the internet and websites around the world through one or more web browsers.

Defendants

10. Defendant CELL NATION OF 3006 BROADWAY CORP. ("CELL NATION") is a corporation organized under the laws of New York with its principal place of business in Astoria, NY. CELL NATION is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

11. Defendant AKRAM INVESTMENTS, LLC ("AKRAM INVESTMENTS") is a limited liability company organized under the laws of Florida with its principal place of business in Altamonte Springs, FL. AKRAM INVESTMENTS is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

12. Defendant INSTA MOBILITY, INC. ("INSTA MOBILITY") is a corporation organized under the laws of Florida with its principal place of business in Belleview, FL. INSTA MOBILITY is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

13. Defendant MELBER, LLC d/b/a HELLO UNLIMITED ("HELLO UNLIMITED") is a limited liability company organized under the laws of Oklahoma with its principal place of business in Oklahoma City, OK. HELLO UNLIMITED is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

14. Defendant LAXCA DF, INC. d/b/a FIVESTONE WIRELESS a/k/a DF WIRELESS ("FIVESTONE WIRELESS") is a company organized under the laws of California with its principal place of business in Walnut, CA. FIVESTONE WIRELESS is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

15. Defendant WIRELESS PCS METRO STATIONS, INC. ("WIRELESS PCS METRO") is a corporation organized under the laws of California with its principal place of business in Chino, CA. Among its storefront locations is a store in Corona, CA. Defendant WIRELESS PCS METRO is a Metro by T-Mobile Authorized Dealer that operates under the Metro by T-Mobile brand.

Other Liable Persons/Entities

16. Plaintiff is prosecuting against Metro by T-Mobile in the private arbitration forum required by Metro by T-Mobile's Terms and Conditions of Service (American Arbitration Association) her claims for the liability Metro by T-Mobile bears for its insiders' acts and omissions in connection with the appalling harm inflicted upon Plaintiff. Should Metro by T-Mobile agree to waive its insistence that Plaintiff's claim be hidden from public scrutiny -- or should the arbitrator presiding over that proceeding declare unconscionable or void as against public policy Metro by T-Mobile's Terms and Conditions of Service (including its requirement that claims such as Plaintiff's be arbitrated) -- Plaintiff will join Metro by T-Mobile as a defendant in the instant matter.

17. Additionally, Plaintiff is prosecuting against an unknown John Doe defendant -- who is believed to have been the thief who stole her cryptocurrency -- in this Court claims seeking damages

and the return of her stolen cryptocurrency assets. *See*, Tullia Heissenberg v. John Doe, U.S. District Court - S.D. Florida - Case No. 9:21-cv-80716-ALTMAN/Brannon.

18. Along with Defendants, Metro by T-Mobile, and John Doe, there are likely other parties who may be liable to Plaintiff, but about whom Plaintiff currently lacks specific facts to permit her to name these persons or entities as party defendants. By not naming such persons or entities at this time, Plaintiff is not waiving her right to amend this pleading to add such parties, should the facts warrant adding such parties.

JURISDICTION AND VENUE

19. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, because the matter in controversy arises under the laws of the United States.

20. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendants because they: (a) conduct business in this jurisdiction, and (b) committed a tort upon Plaintiff in this jurisdiction.

22. Venue of this action is proper in this Court pursuant to 28 U.S.C. § 1391 because the causes of action accrued in this jurisdiction.

GENERAL FACTUAL ALLEGATIONS

Metro by T-Mobile's Business, Authorized Dealer Stores, and Customer Assurances

23. Metro by T-Mobile is a wholly-owned subsidiary of T-Mobile USA, Inc., which is the United States operating entity of T-Mobile International A.G. & Co., the mobile communications subsidiary of Deutsche Telekom AG & Co. K.G. Metro by T-Mobile provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands.

24. Metro by T-Mobile markets and sells wireless telephone service through standardized wireless service plans at various retail locations, online, and over the telephone.

25. Among the retail locations at which accountholders can get customer service in person are: (1) T-Mobile/Metro corporate-owned stores, and (2) Authorized Dealer stores. To accountholders, the difference between the two is functionally imperceptible. Both kinds of stores share inventory with one another, use the same computer systems and databases, market themselves under the T-Mobile/Metro brand, and obtain corporate training from T-Mobile/Metro together. All Defendants in the instant matter operate Metro by T-Mobile Authorized Dealer stores.

26. In connection with its wireless services, Metro by T-Mobile maintains wireless accounts enabling its customers to have access to information about the services they purchase from Metro by T-Mobile. That access is available at Metro by T-Mobile Authorized Dealer stores just as it is available at Metro by T-Mobile Authorized Dealer corporate-owned stores.

27. It is widely recognized that mishandling of customer wireless accounts can facilitate identify theft and related consumer harms.

28. Among other things, Metro by T-Mobile's sales and marking materials state: "**We have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information.**" (Emphasis added).

29. Metro by T-Mobile's sales and marking materials further state that, unless Metro by T-Mobile can verify someone's identity through certain personal information or a PIN if requested by the customer, Metro by T-Mobile's policy is not to release any account-specific information.

> **Verification of Your Identity** We have to verify your identity before we can give you access to or delete your personal data. If we can't verify your identity, we'll unfortunately have to deny your request. This is to protect you. To learn more about our verification process, please read our FAQs. Enterprise customer accounts (T-Mobile for Business/ T-Mobile for Government) are protected through authentication and access methods that are different than those used by individual consumers.

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

30. Despite these statements and other similar statements, Metro by T-Mobile Authorized Dealer stores -- much like Metro by T-Mobile corporate-owned stores themselves -- often fail to provide reasonable and appropriate security to prevent unauthorized access to customer accounts.

31. Under Metro by T-Mobile's procedures, an unauthorized person -- including Metro by T-Mobile Authorized Dealers' own agents and employees acting without the customer's permission -- can easily impersonate the identity of the accountholder and then access and make changes to all the information that a legitimate customer could access and to which the customer could make changes if the customer were so authorized. For example, a simple Google search may reveal the information used to verify the identity of an accountholder, such as an address, ZIP Code, telephone number, and/or e-mail address.

How SIM Swapping Works

32. "SIM swapping," or "SIM hijacking" is a growing crime in the telecommunications world that requires little more than a thorough Google search, a willing telecommunications carrier representative, and an electronic or in-person impersonation of the victim.

33. To activate a mobile device for use on cellular telephone networks, many devices were assigned a unique International Mobile Equipment Identity ("IMEI") number in combination with a unique Subscriber Identity Module ("SIM"), enclosed on a small removable chip or directly embedded into the mobile device. This IMEI/SIM combination -- when paired with a customer's mobile telephone number assigned by a telecommunications carrier -- allows a given user to authenticate on a mobile phone carrier's network to make and receive cellular calls and text messages associated with the customer's mobile telephone number.

34. Generally, "SIM swapping" refers to a method of unauthorized takeover of a victim's wireless account by malicious actors, carried out by linking the victim's mobile telephone number to a SIM card installed in a device controlled by the attacker(s). A typical SIM swap is illustrated below:

35. SIM swaps are commonly executed by attackers who gain unauthorized access to a wireless provider's computer networks or who gain such access with the assistance of witting or unwitting individuals who had access to the telecommunications provider's networks.

36. Often working in tandem with a telecommunications provider's employees and authorized agents -- who sometimes purposefully leak consumer data to third parties and/or the internet as a whole -- an unauthorized person contacts the telecommunications provider's technical support department on the phone, or walks into a telecommunications provider's retail store, intent on assuming the electronic identity of the target of the crime by possessing and utilizing information that only the telecommunications provider should have.

37. By getting the target's wireless telephone number transferred to a new SIM card that he owns, the thief works with the telecommunications provider to utilize the information provided to

him by the telecommunications provider and/or to simply **bypass all security measures** in place on the accountholder's account to effectuate the transfer.

38. Whether acting as a co-conspirator to the theft or through willful and/or abject negligence, the telecommunications provider transfers (or "ports") to the unauthorized person the accountholder's wireless telephone number -- disconnecting the telephone number from the actual accountholder's wireless phone's SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

39. As discussed above, in some cases, upon information and belief, telecommunications provider employees and authorized agents also provide the thief sacrosanct personal information about the targeted accountholder, including his/her security PIN code(s) and his electronic mail address. That information is critical to effectuating the SIM swap.

40. From there, the victim loses cellphone service (including the ability to send or receive talk, text, or data transmissions), given that only one SIM card can be connected to the telecommunications provider's network with any given telephone number at a time.

41. As a result of the SIM swap, phone calls and SMS text messages sent to the victim's mobile telephone number are routed to a device controlled by the attacker(s), giving the attacker(s) complete control over the victim's mobile telephone number.

42. Using the information provided by the telecommunications provider insider(s), the thief then assumes the victim's electronic identity, beginning with his/her electronic mail address, which the thief overtakes employing a simple "Password Reset" feature that requires control of the victim's cellphone number (which was supplied to the thief by the telecommunications provider insider[s]).

43. Having been delivered the victim's cellular telephone number and, directly or indirectly, his/her electronic mail address, the thief then diverts to himself access to the victim's

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

banking and investment accounts (including cryptocurrency holdings) by similarly using the victim's cellular telephone number as a "recovery method" to reset passwords and access to those accounts -- even if the victim had two-factor authentication activated as a security measure on his/her accounts.

44. At that point, the thief absconds with the victim's cryptocurrency holdings and other personal assets.

45. To be clear, simply *knowing* an accountholder's cellphone number or e-mail address is not enough. The key is having **control** over and securing those vital electronic gateways to information and communication; and telecommunications providers regularly and contumaciously place the keys to those gates directly into the hands of unauthorized persons while simultaneously denying their accountholders their power over such things.

The Anatomy of Plaintiff's SIM Swaps

46. In the instant matter, insiders at the defendant Metro by T-Mobile Authorized Dealers -- whether acting as a co-conspirators to the theft or through abject negligence -- transferred to an unknown John Doe control over Plaintiff's mobile telephone number and e-mail address, which **on its seventh SIM swap** ultimately led to the theft of approximately Three Million Dollars ($3,000,000.00) in cryptocurrency assets from Plaintiff on or about March 1, 2021.

a. The First SIM Swap -- CELL NATION (Astoria, NY)

47. At or about 11:52 p.m. EST on **October 25, 2020**, a representative(s) of Metro by T-Mobile Authorized Dealer CELL NATION in Astoria, NY bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

48. Plaintiff went to a T-Mobile corporate store near her home in Delray Beach, FL to explain her problem and express her frustration with the unauthorized transfer of her cellular phone service.

49. At Plaintiff's insistence, Metro by T-Mobile changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

50. Metro by T-Mobile also assured Plaintiff at that time that additional security measures would be implemented on Plaintiff's Metro by T-Mobile account to prevent future unauthorized activity or SIM card swapping. Among the changes made were implementation of a longer PIN on Plaintiff's Metro by T-Mobile account and Metro by T-Mobile's explicit assurance to Plaintiff that no changes could be made over the telephone. Plaintiff was told by Metro by T-Mobile that she would be afforded the highest level of security on her account and that no future SIM transfers would be allowed unless the request were made in a Metro by T-Mobile store and the person making the request were fully vetted with proper identification.

51. Those promises of safety and security rang entirely hollow, as the SIM swaps targeting Plaintiff were just getting started.

b. <u>The Second SIM Swap -- AKRAM INVESTMENTS (Orlando, FL)</u>

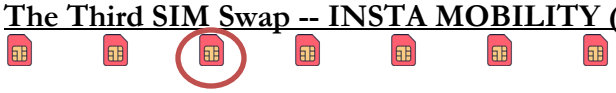
52. On **December 10, 2020**, a representative(s) of Metro by T-Mobile Authorized Dealer AKRAM INVESTMENTS in Orlando, FL bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

53. Plaintiff went to a T-Mobile corporate store near her home in Delray Beach, FL (which is nearly 200 miles from Orlando, FL) to explain her problem and express her frustration with the unauthorized transfer of her cellular phone service.

54. At Plaintiff's insistence, Metro by T-Mobile again changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

55. Metro by T-Mobile also assured Plaintiff at that time that additional security measures would be implemented on Plaintiff's Metro by T-Mobile account to prevent future unauthorized activity or SIM card swapping. Plaintiff was again told by Metro by T-Mobile that she would be afforded the highest level of security on her account and that no future unauthorized SIM transfers would be allowed.

c. The Third SIM Swap -- INSTA MOBILITY (Orlando, FL)



56. On **December 17, 2020**, a representative(s) of Metro by T-Mobile Authorized Dealer INSTA MOBILITY in Orlando, FL bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

57. Plaintiff went to a T-Mobile corporate store near her home in Delray Beach, FL (which is nearly 200 miles from Orlando, FL) to explain her problem and express her frustration with the unauthorized transfer of her cellular phone service.

58. At Plaintiff's insistence, Metro by T-Mobile again changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

59. Plaintiff was again told by Metro by T-Mobile that she would be afforded the highest level of security on her account and that no future unauthorized SIM transfers would be allowed.

d. The Fourth SIM Swap -- HELLO UNLIMITED (Oklahoma City, OK)

60. At or about 1:58 p.m. EST on **January 31, 2021**, a representative(s) of Metro by T-Mobile Authorized Dealer HELLO UNLIMITED in Oklahoma City, OK again bypassed Metro by

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

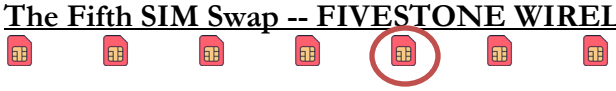
T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

61. Plaintiff again went to a T-Mobile corporate store near her home in Delray Beach, FL to again express her frustration with the unauthorized transfer of her cellular phone service that violated all of the advanced security protocols that had been promised to her by Metro by T-Mobile.

62. At Plaintiff's insistence, Metro by T-Mobile again changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

63. Plaintiff also changed the security code on her Metro by T-Mobile account to a new secure code, described to her by the Metro by T-Mobile representative at that time as a "high security key."

e. <u>The Fifth SIM Swap -- FIVESTONE WIRELESS (El Monte, CA)</u>



64. At or about 2:26 a.m. EST on **February 5, 2021**, a representative(s) of Metro by T-Mobile Authorized Dealer FIVESTONE WIRELESS in El Monte, CA again bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

65. No Metro by T-Mobile Authorized Dealer store (including FIVESTONE WIRELESS) was open at that hour, so the SIM transfer obviously could not have been authorized in-person with properly verified identification -- as required by the enhanced security protocols implemented by Metro by T-Mobile on Plaintiff's account.

66. Once more, Plaintiff went to a T-Mobile corporate store near her home in Delray Beach, FL to remedy the situation; and once more, at Plaintiff's insistence, Metro by T-Mobile changed the SIM card number back to Plaintiff's cellphone, restoring her phone service.

67. Plaintiff again changed the security code on her Metro by T-Mobile account to a new secure code and was assured by a Metro by T-Mobile representative that Plaintiff was "totally safe."

f. The Sixth and Seventh SIM Swaps -- WIRELESS PCS METRO (Corona, CA) and HELLO UNLIMITED (Norman, OK)

68. At or about 4:49 a.m. EST on **February 26, 2021** and at about 12:50 a.m. EST on **February 27, 2021**, representatives of Metro by T-Mobile Authorized Dealer WIRELESS PCS METRO (in Corona, CA) and HELLO UNLIMITED (in Norman, OK), respectively, again bypassed Metro by T-Mobile's security protocols and transferred to an unauthorized person Plaintiff's wireless telephone number -- disconnecting the telephone number from Plaintiff's wireless phone's SIM card in Florida and then connecting the telephone number to a SIM card under the control of the unauthorized person.

69. No Metro by T-Mobile Authorized Dealer store was open at those hours (including WIRELESS PCS METRO and HELLO UNLIMITED), so the SIM transfer obviously could not have been authorized in-person with properly verified identification -- as required by the enhanced security protocols implemented by Metro by T-Mobile on Plaintiff's account.

John Doe's Theft of Plaintiff's Cryptocurrency Holdings

70. Provided access by Defendants' employees or authorized agents, John Doe -- working with those employees and/or agents -- was able to access Plaintiff's cellphone and Plaintiff's account at cryptocurrency exchange BlockFi, where Plaintiff stored a valuable cryptocurrency portfolio.

71. Each Defendant named above worked together to allow John Doe (who may or may not be an employee or authorized agent of one of the Defendants) to maliciously gain access to

Plaintiff's personal identifying information, confidential information of hers stored on the Metro by T-Mobile network, and her cryptocurrency accounts.

72. Commencing on or about March 1, 2021 at 20:01 UTC, John Doe withdrew from Plaintiff's BlockFi account the following cryptocurrency assets -- all without Plaintiff's knowledge or authorization -- and deposited those stolen assets into two cryptocurrency wallets owned or controlled by or for JOHN DOE: bc1qdjkc4e3u8jup6axtda560z720vapq5p34pmwgu (the "John Doe BTC Wallet") and 0xC51f0cbf92030F50829B244f8D876d5843b8A955 (the "John Doe ETH Wallet") (collectively, the "JOHN DOE Wallet Addresses"), *to wit*:

#	Transfer Date (UTC)	Asset sent to John Doe Wallet Address or Fee Charged	JOHN DOE Wallet Address
1	2021-03-01 20:01:47Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
2	2021-03-01 20:01:47Z	0.0025 BTC Withdrawal Fee	
3	2021-03-01 20:01:52Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
4	2021-03-01 20:01:52Z	0.0015 ETH Withdrawal Fee	
5	2021-03-01 20:01:54Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
6	2021-03-01 20:01:54Z	0.0015 ETH Withdrawal Fee	
7	2021-03-01 20:01:56Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
8	2021-03-01 20:01:56Z	0.0015 ETH Withdrawal Fee	
9	2021-03-01 20:01:59Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
10	2021-03-01 20:01:59Z	0.0015 ETH Withdrawal Fee	

11	2021-03-01 20:02:01Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
12	2021-03-01 20:02:01Z	0.0015 ETH Withdrawal Fee	
13	2021-03-01 20:02:04Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
14	2021-03-01 20:02:04Z	0.0015 ETH Withdrawal Fee	
15	2021-03-01 20:02:16Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
16	2021-03-01 20:02:16Z	0.0015 ETH Withdrawal Fee	
17	2021-03-01 20:02:18Z	99.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
18	2021-03-01 20:02:18Z	0.0015 ETH Withdrawal Fee	
19	2021-03-01 20:02:45Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
20	2021-03-01 20:02:45Z	0.0025 BTC Withdrawal Fee	
21	2021-03-01 20:03:06Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
22	2021-03-01 20:03:06Z	0.0025 BTC Withdrawal Fee	
23	2021-03-01 20:03:32Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
24	2021-03-01 20:03:32Z	0.0015 ETH Withdrawal Fee	
25	2021-03-01 20:03:39Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
26	2021-03-01 20:03:39Z	0.0015 ETH Withdrawal Fee	
27	2021-03-01 20:03:43Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
28	2021-03-01 20:03:43Z	0.0015 ETH Withdrawal Fee	
29	2021-03-01 20:03:45Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

30	2021-03-01 20:03:45Z	0.0015 ETH Withdrawal Fee	
31	2021-03-01 20:03:47Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
32	2021-03-01 20:03:47Z	0.0015 ETH Withdrawal Fee	
33	2021-03-01 20:03:49Z	49.9985 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955
34	2021-03-01 20:03:49Z	0.0015 ETH Withdrawal Fee	
35	2021-03-01 20:04:16Z	5 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
36	2021-03-01 20:05:08Z	4.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
37	2021-03-01 20:05:08Z	0.0025 BTC Withdrawal Fee	
38	2021-03-01 20:40:19Z	2.9975 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
39	2021-03-01 20:40:19Z	0.0025 BTC Withdrawal Fee	
40	2021-03-03 21:53:20Z	0.024 BTC	bc1qdjkc4e3u8jup6axtda560z 720vapq5p34pmwgu
41	2021-03-03 21:53:20Z	0.0025 BTC Withdrawal Fee	
42	2021-03-03 22:54:50Z	8 ETH	0xC51f0cbf92030F50829B244 f8D876d5843b8A955

TOTALS	**28.0265 BTC**
	1108 ETH

73. As shown above, with almost every unauthorized withdrawal by John Doe, Plaintiff's BlockFi account was assessed a withdrawal fee that further diminished Plaintiff's cryptocurrency holdings. In essence, the cryptocurrencies from Plaintiff's BlockFi holdings that were used to pay the withdrawal fees were likewise stolen from Plaintiff, as they were forcibly taken from her without her knowledge or authorization.

74. From the John Doe Wallet Addresses, many of the stolen assets were then transferred to other wallets/accounts maintained by or for JOHN DOE (collectively, the "John Doe Secondary Addresses"), *to wit*:

#	Recipient Cryptocurrency Exchange	Destination Address	Asset and Tracing Amount
1		bc1qfwxkmzln5g3g0n8vw5dqsv4vtxumh5xscyzr9l	4.777099848 BTC
2		bc1qkjhlymppxz4g4h6xle8u6scd8d6tm8s657zqqy	3.401842272 BTC
3	Xapo.com	19JyAkHKh36sFduqK4hMsMZhU6ZDoLotW	2.33906575 BTC
4		13jWBgfYQRs1pPwsWhk9jtvjfDMgdByknP	2.20246077 BTC
5		bc1qe8esnkcwyvnnfe5f3ksfmj9eyktq9u0635lhuv	1.478941262 BTC
6		327uTRES6ThXupKUAt1Xuk2pD9BiZaZ4wT	1.10657357 BTC
7	BitPay	15oRB2myPpq8h1jTdRDKE58WXPpSYgK6Qr	1.105248136 BTC
8	Poloniex	12vZ3fU66g4XTeomUYCEPp9rcsWjexgzR7	0.497294128 BTC
9	Binance	15cxBdcNYsdkTW6JoM3Q4xshRF6x8vYrEc	0.41288896 BTC
10	Coinbase	3LF1XGESznTATC7dMQ2zWmZdf4WEJCcehj	0.3 BTC
11	Gemini	bc1qss5ejcqfrmjm9lfydshanhjkc7wnlhk4khlsj8	0.250298812 BTC
12	Binance	e86433d2068bd319a54128117849b511f3e0ed42	1091.1566815047 ETH
13	Coincheck	24ba1542f8a0a20e8251d096213384cfb0ee3dbc	6.322870267 ETH
14		0c32245e86764a61de9feaad1315ac7ceaac70b2	0.0135378573 ETH
15		85dbca0a9bfee831f266065b6142f9ed3b5b1dd7	7.9214341878 ETH
16		a1b78d4c51c50f30c936c3f941c2e206b71b3983	0.0005026098 ETH
17		f7dddfbdb3ea8e0cadf101f37fe08695a955e25c	0.0180210793 ETH
18	Binance	bfaa724c8fc49e490947e4c7c8d597b6336b67ac	0.621182859 ETH
19		2fbbfe6e64d55168cf1ccfc993e61f2c4aa1ef06	0.0239687943 ETH
20		9b5b25216601f065aacbe8e641fa897163a69c2b	1.6162668327 ETH
21		6da237bb6942e5d807a5ac55e7d17e487688d5ee	0.0329650529 ETH
22		31385d3520bced94f77aae104b406994d8f2168c	0.0100385744 ETH

TOTALS	**17.87171351 BTC**
	1107.73746962 ETH

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

75. As of the date(s) on which they were taken from her, the 28.0265 BTC and 1108 ETH stolen from Plaintiff were valued at approximately Three Million Dollars ($3,000,000.00).

76. As a result of the actions described above, Plaintiff has suffered damages in an amount that will be proven at trial.

77. Plaintiff duly performed all of her duties and obligations; and any conditions precedent to Plaintiff bringing this action have occurred, have been performed, or else have been excused or waived.

78. To enforce her rights, Plaintiff has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services.

COUNT I – BREACH OF FEDERAL COMMUNICATIONS ACT [47 U.S.C. §§ 206, 222] (UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION)

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

79. Metro by T-Mobile is a "common carrier" engaging in interstate commerce by wire regulated by the Federal Communications Act ("FCA") and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

80. Defendants are each authorized agents of common carrier Metro by T-Mobile and, under section 217 of the FCA [47 U.S.C. § 217], are themselves liable for adhering to the requirements of the FCA as well as their violations of the FCA.

81. Under section 206 of the FCA [47 U.S.C. § 206], "[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a

reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case."

82. Section 222(a) of the FCA [47 U.S.C. § 222(a)] requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers ("CPI").

83. Section 222(c)(1) of the FCA [27 U.S.C. § 222(c)(1)] further requires that, "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information ['CPNI'] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services . . . ."

84. The information disclosed to hackers by Defendants in the 2020-2021 SIM swap frauds transferring Plaintiff's telephone number was CPI and CPNI under Section 222 of the FCA.

85. Defendants failed to protect the confidentiality of Plaintiff's CPI and CPNI, including her wireless telephone number, account information, and her private communications, by divulging that information to hackers multiple times -- the latest time being on February 27, 2021.

86. Through their negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the warnings of the Pretexting Order, its Privacy Policy, COBC, and CPNI Policy, and by allowing its employees to bypass such procedures, Defendants permitted hackers to access Plaintiff's telephone number, telephone calls, text messages and account information to steal approximately $3,000,000.00 worth of her cryptocurrency.

87. As a direct consequence of Defendants' violations of the FCA, Plaintiff has been damaged by loss of approximately $3,000,000.00 worth in cryptocurrency which Defendants allowed

to fall into the hands of thieves, and for other damages in an amount to be proven at trial in this matter.

88. Plaintiff is also entitled to her attorney's fees under the FCA in bringing this action against Defendants for their gross negligence and fraudulent misrepresentation as to the security that they were obligated to provide for customer accounts as required by the FCA and the CPNI Regulation.

COUNT II – VIOLATION OF FLA. STAT. § 415.1111
(ADULT PROTECTIVE SERVICES ACT - ELDER EXPLOITATION)

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 78 above, and further alleges:

89. This cause of action asserts a claim against Defendants for violations of Fla. Stat. § 415.1111 (Florida's "Adult Protective Services Act") for exploiting Plaintiff and for aiding and abetting the theft, conversion, and misappropriation of Plaintiff's cryptocurrency assets in a manner that deprived Plaintiff of, and infringed upon, her rights.

90. Plaintiff is a "vulnerable adult," as that term is defined in Fla. Stat. § 415.102(28).

91. Plaintiff has been exploited by, and has a civil cause of action against, Defendants for the harm they have inflicted upon her.

92. Not only have Defendants inflicted upon Plaintiff numerous unauthorized SIM swaps by divulging to unauthorized parties Plaintiff's personal identifying information and by violating numerous security protocols and assurances of safety and security that they made to Plaintiff, Defendants have also aided and abetted the unknown person who obtained and absconded with Plaintiff's cryptocurrency assets through acts of theft, fraud, conversion, and misappropriation.

93. Pursuant to Fla. Stat. § 415.1111, Plaintiff is entitled to recover from Defendants actual damages, punitive damages, reasonable attorney's fees, and the costs of this action.

COUNT III – VIOLATION OF 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4)
(COMPUTER FRAUD AND ABUSE ACT ["CFAA"])

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

94. This cause of action asserts a claim against Defendants for violations of 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4) (the "Computer Fraud and Abuse Act") for aiding and abetting authorized access to a protected computer to obtain information, for knowingly doing so with an intent to defraud, and for furthering fraudulent activity thereby to obtain something of value.

95. Plaintiff's cellphone is a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) because it is used in interstate or foreign commerce or communication, including sending and receiving electronic mail, sending and receiving text messages, and accessing and interacting with the internet.

96. Defendants aided and abetted an unauthorized and unknown person by granting to that person, acting knowingly and with intent to defraud Plaintiff, access to a protected computer (*i.e.*, Plaintiff's cellphone).

97. Defendants divulged to an unauthorized person Plaintiff's personal identifying information -- including her private security PIN codes -- and transferred to that unauthorized person Plaintiff's cellphone number and the telecommunications services tied thereto through Plaintiff's cellphone.

98. Defendants aided and abetted the unauthorized transfer of Plaintiff's SIM card despite the clear barrier of numerous security protocols on Plaintiff's account that Defendants overtly ignored and bypassed -- a barrier that Defendants expressly represented to Plaintiff was put in place to prevent an unauthorized SIM swap.

99. As a consequence of Defendants' actions and omissions, Plaintiff has suffered damage far in excess of Five Thousand Dollars ($5,000.00).

100. Moreover, as a consequence of Defendants interrupting Plaintiff's service, she has suffered damage far in excess of Five Thousand Dollars ($5,000.00).

COUNT IV – VIOLATION OF 18 U.S.C. § 1030(a)(6)
(COMPUTER FRAUD AND ABUSE ACT ["CFAA"])

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

101. This cause of action asserts a claim against Defendants for violations of 18 U.S.C. § 1030(a)(6) (the "Computer Fraud and Abuse Act") for knowingly and with an intent to defraud trafficking in Plaintiff's password or similar information through which a computer may be accessed without authorization where such trafficking affects interstate commerce.

102. Defendants knowingly, and with intent to defraud Plaintiff, trafficked in Plaintiff's password or similar information by giving Plaintiff's security passcode to an unauthorized third party.

103. Using Plaintiff's passcode, the unauthorized third party was able to access Plaintiff's computer (*i.e.*, her cellphone) without Plaintiff's authorization.

104. The unauthorized access to Plaintiff's cellphone affects interstate commerce, as the phone can be used -- and is regularly used -- as a tool to make interstate phone calls, access the internet for the purchase and sale of goods and services, and transmit text and data across state lines using electronic mail and text messaging services.

105. As a consequence of the conduct described above -- and because Defendants interrupted Plaintiff's service during a critical timeframe -- Plaintiff has suffered damage.

COUNT V – VIOLATION OF FLA. STAT. §§ 815.01, *et seq.*
(FLORIDA COMPUTER CRIMES ACT)

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

106. This cause of action asserts a claim against Defendants for violations of Fla. Stat. §§ 815.01, *et seq.* (the Florida Computer Crimes Act ["the Act"]) for aiding and abetting unlawful access

to Plaintiff's Metro by T-Mobile cellphone and for disrupting and denying Plaintiff's Metro by T-Mobile service in a manner that allowed the theft of her cryptocurrency assets.

107. Fla. Stat. § 815.06 deems a person to have committed an offense under the Act if he/she/it, *inter alia*:

> (a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized . . . .
>
> (b) Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another.

108. Furthermore, Fla. Stat. § 815.06 provides a civil right of action to someone aggrieved by a violation of any provision of the Act; and the aggrieved person is authorized to sue therefor and recover compensatory damages as well as reasonable attorneys' fees incurred.

109. Under Fla. Stat. § 815.03(4), the wireless telecommunications network for which Plaintiff paid a monthly subscription to access from Metro by T-Mobile is deemed a "computer network."

110. Under Fla. Stat. § 815.03(6), the wireless telecommunications services for which Plaintiff paid a monthly subscription to Metro by T-Mobile are deemed "computer services."

111. Under Fla. Stat. § 815.03(9), Plaintiff's cellphone is deemed an "electronic device."

112. At the time Defendants handed over to an unauthorized person Plaintiff's cellphone number, Plaintiff's password, an identifying code, Plaintiff's personal identification number, or other confidential information and control over Plaintiff's cellular telephone services, Defendants not only allowed the unauthorized person access to Plaintiff's cellular telephone services but also prevented Plaintiff's authorized access to those same services during the critical time period in which the theft of Plaintiff's assets took place.

113. To the extent Defendants did not commit primary violations of this statute, Defendants provided vital assistance and aided and abetted violation of the statute by the unauthorized person -- who did so knowingly and without authorization or without reasonable grounds to believe that he or she had such authorization to access Plaintiff's cellular telephone.

114. Through their knowing cooperation with the hacker in the SIM swap fraud, Defendants provided the hacker with means to access Plaintiff's cellphone to steal nearly $3,000,000.00 worth of cryptocurrency from Plaintiff.

COUNT VI – NEGLIGENCE

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

115. Defendants owed a duty to Plaintiff to exercise reasonable care in safeguarding and protecting her Personal Information, including CPI and CPNI, and keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

116. This duty included, among other things, designing, maintaining, and testing their security systems to ensure that Plaintiff's Personal Information, including CPI and CPNI, was adequately secured and protected.

117. Defendants knew that Plaintiff's Personal Information, including CPI and CPNI, was confidential and sensitive.

118. Indeed, Metro by T-Mobile acknowledged this in its Privacy Policy, COBC, and CPNI Policy.

119. Defendants likewise knew that Plaintiff's Personal Information was vulnerable to hacks by thieves and other criminals both because Metro by T-Mobile acknowledged such in its Privacy Policy, COBC, and CPNI Policy and because they had been informed by Plaintiff of the multiple hacks into her Metro by T-Mobile account prior to February 28, 2021.

120. Defendants thus knew of the substantial and foreseeable harms that could occur to Plaintiff if they did not place adequate security on her Personal Information and did not follow their own security measures for the account.

121. By being entrusted by Plaintiff to safeguard her Personal Information, including CPI and CPNI, Defendants had a special relationship with Plaintiff.

122. Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide her Personal Information to Metro by T-Mobile with the understanding that Metro by T-Mobile would take appropriate measures to protect it. But Defendants -- acting as authorized agents of Metro by T-Mobile -- did not protect Plaintiff's Personal Information and violated her trust.

123. Defendants knew their security was inadequate.

124. Defendants are morally culpable, given prior security breaches involving their own employees.

125. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, the CPNI Rules, and its own Privacy Policy, COBC, and CPNI Policy.

126. Defendants' failure to comply with federal and state requirements for security further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI.

127. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff, her Personal Information, including her CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons.

128. Defendants' negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of her resulting damages, including, but not limited to, the theft of approximately $3,000,000.00 worth of cryptocurrency.

129. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including her CPI and CPNI.

130. Defendants' misconduct as alleged herein is malice, fraud, or oppression in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of her rights.

131. As a result, Plaintiff is entitled to punitive damages against Defendants.

COUNT VII – NEGLIGENT MISREPRESENTATION

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

132. Defendants made numerous representations and false promises to Plaintiff of security and compliance with Metro by T-Mobile's Privacy Policy, COBC, and CPNI Policy as well as its advertising regarding the supposed security of consumers' Personal Information, including Plaintiff's Personal Information.

133. Such representations and promises were false because Defendants -- as authorized agents of Metro by T-Mobile -- were using outdated security procedures and failed to disclose that they did not adhere to Metro by T-Mobile's own standards, including the security standards that were purportedly implemented for Plaintiff in or prior to February 2021 or the CPNI Rules.

134. Defendants' misrepresentations and false promises, including those made in or prior to February 2021, were material to Plaintiff, who reasonably relied upon those representations and promises.

SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

135. Plaintiff would not have agreed to continue to use and pay for Metro by T-Mobile's services if she had known that they were not as secure as represented by Defendants and would not have lost approximately $3,000,000.00.

136. Defendants intended that Plaintiff rely on their representations and promises, including those made in or prior to February 2021, as they knew that Plaintiff would not entrust her Personal Information to unreasonable security risks.

137. In reliance upon Defendants' representations and promises, Plaintiff continued to maintain a wireless account with Metro by T-Mobile and to use her Metro by T-Mobile phone number for verification and other purposes.

138. As a direct and proximate result of Defendants' wrongful actions, Plaintiff has been damaged.

COUNT VIII – NEGLIGENT TRAINING AND SUPERVISION

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-78 above, and further alleges:

139. Defendants owed Plaintiff a duty to exercise reasonable care in supervising and training their employees to safeguard and protect Plaintiff's Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

140. Defendants were aware of the ability of their employees to bypass security measures and the fact that their employees actively participated in fraud involving their customers, including pretexting and SIM card swap fraud, by bypassing such security measures.

141. Defendants knew that Plaintiff's Personal Information, including CPI and CPNI, was confidential and sensitive.

142. By being entrusted by Plaintiff to safeguard her Personal Information, including CPI and CPNI, Defendants had a special relationship with Plaintiff.

143. Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide her Personal Information to Metro by T-Mobile with the understanding that Metro by T-Mobile's employees and authorized representatives would take appropriate measures to protect it.

144. Metro by T-Mobile also made promises in the Privacy Policy, COBC, and CPNI Policy that its employees would respect its customers' privacy and that Metro by T-Mobile would supervise and train its employees to adhere to its legal obligations to protect their Personal Information.

145. Defendants breached their duty to supervise and train their employees to safeguard and protect Plaintiff's Personal Information, including CPI and CPNI, by not requiring them to adhere to their obligations under the CPNI Rules and other legal provisions.

146. On no fewer than seven separate occasions, Defendants' employees facilitated SIM swap frauds on Plaintiff by not requiring an individual(s) requesting Plaintiff's telephone number to present valid identification.

147. Defendants knew their supervision and monitoring of their employees was inadequate through their knowledge from prior incidents that their employees cooperated with hackers in SIM swap fraud.

148. Defendants are morally culpable, given prior security breaches involving their own employees.

149. Defendants breached their duty to exercise reasonable care in supervising and monitoring their employees to protect Plaintiff's Personal Information, including CPI and CPNI.

150. Defendants' failure to comply with the requirements of the FCA and CPNI Rules further evidence Defendants' negligence in adequately supervising and monitoring their employees so that they would safeguard and protect Plaintiff's Personal Information, including CPI and CPNI.

151. But for Defendants' wrongful and negligent breach of their duties to supervise and monitor their employees, Plaintiff's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud.

152. Defendants' negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of her resulting damages, including, but not limited to, the theft of approximately $3,000,000.00 worth of cryptocurrency.

153. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendants' failure to supervise and monitor their employees in safeguarding and protecting Plaintiff's Personal Information, including her CPI and CPNI.

154. Defendants' misconduct as alleged here was done with malice, fraud and oppression in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of her rights. As a result, Plaintiff is entitled to punitive damages against Defendants.

COUNT IX – CIVIL CONSPIRACY

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 78 above, and further alleges:

155. Defendants, by and through their authorized agents, agreed and combined with one another and with yet-unknown third-party thieves to engage in a conspiracy to:

(a) violate federal laws, including the Federal Communications Act;

(b) hand over to unauthorized persons Plaintiff's cellphone number, Plaintiff's Metro by T-Mobile password/identifying code, Plaintiff's personal identification number, or other confidential information and control over Plaintiff's cellular telephone services;

(c) overtly and intentionally ignore and bypass numerous security protocols on Plaintiff's account -- barriers expressly represented to Plaintiff that were was put in place to prevent an unauthorized SIM swap;

(d) prevent Plaintiff's authorized access to the Metro by T-Mobile services for which she paid during the critical time period in which the theft of Plaintiff's assets took place; and

(e) represent and support a criminal syndicate aimed at stealing cryptocurrency from Metro by T-Mobile accountholders (including Plaintiff) following unauthorized SIM swaps on those Metro by T-Mobile accountholders.

156. The participants in the conspiracy put their own pecuniary interests ahead of the welfare and economic safety of the victim of this portion of the conspiracy: Plaintiff.

157. Defendants failed to comply with their legal obligations -- and in fact intentionally or through recklessness and gross negligence violated those obligations -- and enabled the illegal activity inflicted upon Plaintiff.

158. Each Defendant acted in concert in furtherance of its role in the common plan to steal, launder, and dissipate cryptocurrency assets from Metro by T-Mobile accountholders, including Plaintiff.

159. As a direct and proximate result of Defendants' participation in, and furtherance of, the conspiracy; Plaintiff has suffered damages.

PRAYER FOR RELIEF

WHEREFORE, Claimant TULLIA HEISSENBERG, an individual, respectfully prays for relief as follows:

(a) A judgment awarding Plaintiff equitable restitution, including, without limitation, restoration of the *status quo ante*, and return to Plaintiff all cryptocurrency or fiat currency taken from her in connection with the SIM card swaps intentionally inflicted or negligently allowed by Defendants;

(b) An award of any and all additional damages recoverable under law including but not limited to compensatory damages, punitive damages, incidental damages, and consequential damages;

(c) Pre- and post-judgment interest;

(d) Attorneys' fees, expenses, and the costs of this action; and

(e) All other and further relief as the Arbitrator deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

RESERVATION OF RIGHTS

Plaintiff reserves her right to further amend this Complaint, upon completion of her investigation and discovery, to assert any additional claims for relief against Defendants or other parties as may be warranted under the circumstances and as allowed by law.

Respectfully submitted,

SILVER MILLER
4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: _____
DAVID C. SILVER
Florida Bar No. 572764
E-mail: DSilver@SilverMillerLaw.com
JASON S. MILLER
Florida Bar No. 072206
E-mail: JMiller@SilverMillerLaw.com

Counsel for Plaintiff Tullia Heissenberg

Dated: November 4, 2022